DYNAMIC JAMMING OF NETWORKS

Final Report

Axiomatix

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION: Unclassified	1b. RESTRICTIVE MARKINGS:
2a. SECURITY CLASSIFICATION AUTHORITY:	3. DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release; distribution unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE:	
4. PERFORMING ORGANIZATION REPORT NUMBER(S): R9003-4	5. MONITORING ORGANIZATION REPORT NUMBER(S): ARO 24649.1-D-EL-S
6a. NAME OF PERFORMING ORGANIZATION: Axiomatix; 6b. OFFICE SYMBOL (If applicable):	7a. NAME OF MONITORING ORGANIZATION: U. S. Army Research Office
6c. ADDRESS (City, State, and ZIP Code): 9841 Airport Blvd., Suite 1130, Los Angeles, CA 90045	7b. ADDRESS (City, State, and ZIP Code): P. O. Box 12211, Research Triangle Park, NC 27709-2211
8a. NAME OF FUNDING/SPONSORING ORGANIZATION: U. S. Army Research Office; 8b. OFFICE SYMBOL (If applicable):	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER: DAAL03-87-C-0007
8c. ADDRESS (City, State, and ZIP Code): P. O. Box 12211, Research Triangle Park, NC 27709-2211	10. SOURCE OF FUNDING NUMBERS: PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO

11. TITLE (Include Security Classification): DYNAMIC JAMMING OF NETWORKS

12. PERSONAL AUTHOR(S): Andreas Polydoros, Gaylord K. Huth, and Unjeng Cheng

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Final	FROM 4/15/87 TO 4/15/90	1990, March 31	10

16. SUPPLEMENTARY NOTATION: The view, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy, or decision, unless so designated by other documentation.

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number): Code-Division-Multiple-Access (CDMA), Communications, Frequency-Hopping, Networks, Packet Radio, Spread Spectrum, Temporal-Selective Jamming, Topology-Selective Jamming.

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The problem addressed in this report is the intelligent, topology-selective jamming of spread-spectrum networks. The key goal has been to develop analytical and simulation tools which quantify the effect of jamming strategies upon the network operation, both at the link-access and the end-to-end layer. The purpose of these tools (called herein "the AJ network analyzer") is to help study the tradeoffs between the jammers' strategies and choices, versus the corresponding choices of the communicators (users). An important feature of the analyzer is the modular incorporation of any jammer/user interaction at the physical (waveform) level within the analyzer framework, so that a variety of modulation/coding/spreading/jamming formats could be studied with regard to their impact upon the higher-layer performance measures.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT: ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION: Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL: Dr. Gaylord K. Huth	22b. TELEPHONE (Include Area Code): (213) 641-8600; 22c. OFFICE SYMBOL:

DD FORM 1473, 84 MAR — 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

TABLE OF CONTENTS

Page

1.0 Introduction 1

2.0 Summary of the Most Important Results 2

2.a Summary of Report Findings 4

3.0 Bibliography 8

1.0 STATEMENT OF PROBLEM STUDIED

The problem addressed in this report is the intelligent, topology-selective jamming of spread-spectrum networks. The key goal has been to develop analytical and simulation tools which quantify the effect of jamming strategies upon the network operation, both at the link-access and the end-to-end layer. The purpose of these tools (called herein "the AJ network analyzer") is to help study the tradeoffs between the jammers' strategies and choices, versus the corresponding choices of the communicators (users). An important feature of the analyzer should be the modular incorporation of any jammer/user interaction at the physical (waveform) level within the analyzer framework, so that a variety of modulation/coding/spreading/jamming formats can be studied with regard to their impact upon the higher-layer performance measures. This parametric incorporation of the physical layer would enable the network analyzer to take advantage (in a totally modular way) of the wealth of previously published knowledge about the jamming effects on the signal format.

As detailed in the "statement of work" of our original technical proposal of June 1986, three subtasks would be undertaken within the context of this study. There were phrased as follows:

> (1) We shall develop an AJ network analyzer, which will describe and couple adaptive routing algorithms and dynamic jammer models. Initial computation software will be developed, written in C language.
>
> (2) We shall assess the effectiveness of intelligent dynamic jamming including such choices as topology selection, duty factor, traffic intensity monitoring, follower jammer, etc. We shall recommend communicator's network countermeasures.
>
> (3) We shall perform average and worst-case tradeoff analysis of jammer and communicator alternatives and develop a comprehensive analytical and computation software, which will be verified by simulation.

As we discuss in the following section, "Summary of the Most Important Results," significant progress has been achieved in all these subtasks.

2.0 SUMMARY OF THE MOST IMPORTANT RESULTS

In order to acquire a solid understanding of the various mechanisms by which an intelligent, average-power-constrained, strategy-optimized jammer can affect a spread-spectrum network, it became clear very early into the project that a two-pronged approach needed to be followed: in the first class of problems addressed, we would try to gain an intimate insight into the interplay between the jammer and the users' link-access strategies or protocols. In order to do that, we needed to (a) assume a fully-connected topology, (b) develop novel stochastic jamming models that provide topological selectivity, (c) describe a detailed random-accessing mechanism for the users, and (d) develop an exact analytical model for the stochastic evolution of the combined user-jammer system, which would describe precisely the temporal evolution of the system state (in this case, the number of backlogged users in each slot). This exact analytic tool, despite certain necessary simplifying assumptions that needed to be made in order to make it tractable, proved valuable in assessing certain jammer/user trade-offs and interactions. More details on this part of our study are provided below.

In the second class of problems, the interplay between the end-to-end network aspects (e.g., routing choices) and the jammers' topological choices (i.e., node-jamming selectivity) were addressed. The complicated dependence between a specific network/jammer configuration and the desired performance measure, as well as the significant statistical dependence between the actions of buffered users and the jammer, makes exact analysis quite intractable. Instead, an approximate interactive analytic procedure was advanced for the cases where a static, stationary jamming model allowed the network to reach a stochastic equilibrium. Otherwise, when a static (i.e., no state-feedback employed in the jamming action), non-stationary (i.e., time-varying) jammer was considered, a simulation technique was developed and employed to study specific network/jammer configurations. Here, too, these tools allowed us to gain a quantitative

insight into the interaction between the jammer's topological choices and the users' countermeasures.

In addition to this last case, extensive Monte-Carlo simulation has been employed throughout to substantiate the claims of all exact or approximate analytical efforts. The simulation packages associated with this study are described elsewhere. Our specific philosophy in mixing analytical and simulation models and results emerges, hopefully, in a clear form from the above description: we would initially approach analytically (exactly or approximately) classes of network-jammer combination models for which a stochastic equilibrium (steady-state) can be ascertained. Static, stationary strategies from both sides (users and jammer) usually fit this mode, although the accuracy of approximate analytic procedures needed to be questioned and examined (via simulation) in complex cases. We note that dynamic equilibrium can also be reached for properly designed dynamic procedures (where some sort of feedback-action is employed, based on link or network observables) although we did not address this class of problems analytically in this study. On the other hand, simulation was used exclusively for the much more complicated scenarios, such as the case of a dynamic user-routing procedure in the face of either stationary or non-stationary (periodic, in particular), static (state-independent) jamming strategies. We note that dynamic (state-dependent) jamming techniques were not addressed. In the present context, these dynamic user countermeasures, namely, the adjustment of routing decisions based on link observables or measurements, comprises one aspect of the general notion of network adaptivity; other aspects include power control (i.e., network connectivity), coding adjustment at the transmitter side, adaptive code combining at the receiver side, etc., which are not covered here.

We provide below a brief summary of the findings of the published technical reports of this contract. In order to get the nomenclature straightened out from the beginning, and to avoid confusion over semantics, the reader is encouraged to consult first the Report No. R8912-1 [12], where an elaborate classification of the system structures

and parameters is provided. This should establish a unified terminology for all previous reports, which occasionally differ in terminology, in view of the evolving nature of the project.

The general conclusion of this study so far can be stated in simple terms: there exists a significant interaction, as expected, between the jamming strategies and the associated parameter and topological jamming choices, on one hand, and the adaptive user choices and countermeasures, on the other. The fundamental network performance measures, namely, the information throughput (or utilization) and delay are greatly affected by these mutual choices, either in the average or in the worst-case sense. Robust system operation can be designed and achieved, predicated on some amount of system-level knowledge (average signal-to-jammer power, network size, some routing information, etc.). Nonetheless, many more issues, concepts, techniques and tools need to be addressed and resolved, for which this study can serve both as an identifier as well as a first stepping stone towards that direction.

2.a Summary of Report Findings

R8712-5 [1]. This report addresses the fully-connected network model and introduces novel concepts of stationary, stochastic, topology-selective jamming. Two particular jamming scenarios and examined in detail. The composite user/jammer Markovian model is formulated and analyzed by means of a newly introduced combinatorial algorithm. Numerical results are presented for the case of Direct-Sequence modulation. The impact of the user choice of link-access parameters, coding rate, topology, and parameter optimization is depicted, versus the choice of the key jamming parameter, the spatial jamming factor.

R8712-6 [2]. This report looks at time-invariant jamming attacks on a multihop network via approximate analytic networks. Three particular approaches are adapted to the present jamming environment and compared. It is shown that the Queuing Network Analyzer

(QNA) outperforms the others in approximating the simulated network behavior, although all become loose predictors at high-traffic levels. The basic features of the simulation package are described. Some thoughts on the simulation of the time-varying jamming attack are initiated (this jamming strategy is described as "dynamic" although, in view of the Report No. R8912-1 [12], it should be called "instationary" or "time-varying" (the same goes for subsequent reports).

R8806-1 [5] . This report introduces and describes a simulation package for the study of periodic (special case of time-varying) jamming strategies against an user-adaptive (dynamic) network. The "window-average" and "time-average" techniques are introduced as appropriate vehicles for the average evaluation of the packet delay and node queue sizes, which comprise valid performance measures in the absence of an equilibrium or steady-state for the network. Certain time-varying network features can also be explored, such as the response speed of the adaptive routing algorithm and the time variation of the node traffic intensity. As a result of using the package, the worst-case choice of the period of the periodic jammer can be identified as a function of the jamming topology and the user traffic distribution. The report also identifies important new research problems.

R8812-1 [7]. This report extends the theory in R8712-5 [1] for the important case where the modems in the network are half-duplex instead of dedicated. It is shown that this important feature of network topology (in the fully-connected case) can alter the optimal jamming strategy significantly (i.e., the choice of the spatial duty factor). It also identifies and explains the corresponding optimal choices for the user link-access parameters and compares the system utilization to the dedicated-modem case.

R8906-3 [9]. This report extends the multihop theory of report R8712-6 [2] to the case of a time-varying, aperiodic jammer. The network is disrupted by a sequence of jamming patterns (topological choices), which remain fixed for a period of time (a "block" or

"window") but change from one window to the next. We note that this can model either a deterministic, time-varying jammer, or it can represent a particular temporal profile (sample jamming waveform) of a stationary stochastic jammer who chooses patterns in each block with some prescribed probability. This report is concerned with establishing a block-iterative procedure for an approximate quasi-analytic evaluation of the network, with the QNA algorithm as its core component for performance evaluation on a per-block basis (a short-term type of equilibrium solution in each block). New concepts like the modified traffic, transient nodes and blocked packets are described.

R8912-1 [12]. This report reviews and classifies a variety of concepts, parameters and alternatives in the analysis and design of jammed spread-spectrum networks. It also identifies certain (but not all) directions in which further research would be valuable to the Army in this particular topic.

R9003-2 [14]. This report extends the theory of R8712-5 [1] to the case of Frequency-Hopping MFSK modulation. It is shown that the jammer can choose the spatial duty factor as to inflict a damage (reduction) in the network utilization, up to 50% in certain cases, in comparison to the full-space jammer. For the particular scenario chosen, the spatial duty factor coincides with the temporal duty factor on a per-node basis (probability of the node being jammed in any slot). The optimal jamming probability was found to be about 0.6 in these examples.

R9003-3 [15]. This report described the network simulator with the nonstationary jamming features. The simulator includes both the Direct-Sequence and Frequency-Hopping models. Two propagation loss models are supported, namely, square-law loss and power-of-four-loss. The software is menu-driven and provides a network editor and a jammer topology editor. Using this simulator, we are able to show that a completely-

connected network may become a multi-hop network when the jamming power is strong enough.

SCIENTIFIC PERSONNEL SUPPORTED

Andreas Polydoros	Part-time
Unjeng Cheng	Part-time

Principal Investigator
Gaylord Huth

3.0 BIBLIOGRAPHY

[1] "Topology Selective Jamming of Certain CDMA Monohop Networks," Interim Technical Report, Axiomatix Report No. R8712-5, December 23, 1987.

[2] "Static and Dynamic Jamming of Networks," Interim Technical Report, Axiomatix Report No. R8712-6, December 23, 1987.

[3] "Dynamic Jamming of Networks," Progress Report for July 1, 1987 through December 31, 1987, Axiomatix Report No. R8801-5, January 26, 1988.

[4] A. Polydoros and U. Cheng, "Topology-Selective Jamming of Certain CDMA Monhop Networks," presented at IEEE International Symposium on Information Theory, Kobe, Japan, June 19–24, 1988.

[5] "Simulation Study of Periodic Jamming of Adaptive Network," Interim Technical Report, Axiomatix Report No. R8806-1, June 30, 1988.

[6] "Dynamic Jamming of Networks," Progress Report for January 1, 1988 through June 30, 1988, Axiomatix Report No. R8807-4, July 26, 1988.

[7] "Dedicated vs. Half-Duplex Receiver Topology in Jammed, Fully-connected CDMA Networks: Theory and Numerical Comparisons," Interim Technical Report No. R8812-1, December 23, 1988.

[8] "Dynamic Jamming of Networks," Progress Report for July 1, 1988 through December 31, 1988, Axiomatix Report No. R8901-2, January 17, 1989.

[9] "Network Analyzer for Nonstatic Jamming," Interim Technical Report, Axiomatix Report No. R8906-3, June 30, 1989.

[10] "Dynamic Jamming of Networks," Progress Report for January 1, 1989 through June 30, 1989, Axiomatix Report No. R8907-2, July 22, 1989.

[11] Simulation and Emulation of Dynamic Jamming of the Mobile Subscriber Equipment (MSE)," Interim Technical Report, Axiomatix Report No. R8911-1, November 6, 1989.

[12] "Packet Radio Networks Under Dynamic Jamming," Interim Technical Report, Axiomatix Report No. R8912-1, December 15, 1989.

[13] "Dynamic Jamming of Networks," Progress Report for July 1, 1989 through December 31, 1989, Axiomatix Report No. R9001-1, January 24, 1990.

[14] "Topology-Selective Jamming of Monohop Networks Using Frequency-Hopping MFSK Modulation," Interim Technical Report, Axiomatix Report No. R9003-2, March 31, 1990.

[15] "A Novel Communication Network Simulator," Interim Technical Report, Axiomatix Report No. R9003-3, March 31, 1990.